



DEPARTMENT OF THE ARMY
HEADQUARTERS, MILITARY TRAFFIC MANAGEMENT COMMAND
200 STOVALL STREET HOFFMAN BUILDING 1F
ALEXANDRIA VA 22332-5000

March 14, 2002



Distribution Analysis Center

Munitions Carrier Industry

Policy Letter (PL) 2002-01: PERSONNEL SECURITY CLEARANCE REQUIREMENTS FOR COMMERCIAL CARRIER PERSONNEL INVOLVED IN THE TRANSPORTATION OF DOD ARMS, AMMUNITION AND EXPLOSIVE (AA&E) SHIPMENTS

The Military Traffic Management Command (MTMC) letter dated November 1, 2001 established new security clearance requirements for all carrier employees involved in the movement of Department of Defense (DOD) Arms, Ammunition and Explosives (AA&E). The intent of this letter is to identify the carrier employees that are affected by the new requirements.

The requirement for employees to maintain a "SECRET" personnel security clearance granted by the Defense Security Service shall apply to all drivers transporting DOD AA&E and to any individuals who have access to information relating to a DOD AA&E shipment prior to delivery at final destination. The following employees normally have advance access to information regarding AA&E shipments and therefore shall require a DOD "SECRET" security clearance: Facility Security Officer Terminal Manager Operations Manager Driver / Fleet Manager Dispatcher Router / Load Planner

The following personnel require a "SECRET" clearance if they receive advance notification of information regarding DOD AA&E shipments: Hazardous Material / Compliance Personnel Terminal Personnel Government Sales Representative Computer Programmer/Technician supporting In-transit Shipment Operations Any other personnel having prior knowledge of AA&E shipments

Personnel who normally have knowledge of or access to information relating to DOD AA&E shipments only after delivery are not required to hold a security clearance.

Employees requiring a "SECRET" clearance must complete an Electronic Personnel Security Questionnaire (EPSQ) version 2.2 in accordance with the timelines of our November 1, 2001 letter. Only employees who actually hold a SECRET clearance (interim or final) can transport DOD AA&E after 30 September 2002. Employees who are in process for a clearance after that date but do not hold an interim or final clearance cannot be used for AA&E until they do.

Employee records will be subject to review during authorized terminal inspections. MTMC Operations Center (757-878-7555/8141) will pre-approve access to terminal facilities and records by all inspectors.

As a reminder, the code "9Z" must be entered in the two-digit prioritization field in EPSQ version 2.2, which can be found under the Certify - Certify User Form menu. This will enable tracking of the number of clearance requests associated with this new security requirement.

Future questions and concerns regarding this issue may be addressed to Mr. Mark Gerade, (703) 428-2315, FAX (703) 428-2315, or email: geradem@mtmc.army.mil.

CF:

American Trucking Association, ATTN: Mr. William Wanamaker
HQ, Military Traffic Management Command, ATTN: Operations Center

A handwritten signature in black ink, appearing to read 'F. Galluzzo', followed by a horizontal line.

Francis A. Galluzzo
Director
Distribution Analysis Center



DEPARTMENT OF THE ARMY
HEADQUARTERS, MILITARY TRAFFIC MANAGEMENT COMMAND
200 STOVALL STREET HOFFMAN BUILDING 11
ALEXANDRIA VA 22332-5000



March 14, 2002

Distribution Analysis Center

Munitions Carrier Industry

Policy Letter (PL) No. 2002-02: IN-TRANSIT FACILITY AND TERMINAL REQUIREMENTS FOR HANDLING SMALL QUANTITY AA&E SHIPMENTS, CLASSIFIED AND OTHER SENSITIVE SHIPMENTS

The enclosed standards detail the protection at motor carrier terminals for the following types of shipments moving under the indicated protective services:

Shipment Type

Protective Service(s)

- Small quantity shipments of arms, ammunition and explosives (AA&E) (as defined in DTR, Part 11, Chapter 205, Paragraph G)

DOD Constant Surveillance Service (CIS)

- Classified, non-AA&E shipments

Protective Security Service (PSS) or CIS

- Other sensitive or pilferable, non-AA&E shipments.

Dual Driver Protective Service (DDP) or CIS

These standards are effective April 30, 2002 and will remain in effect until further notice.

Terminal safety and security standards for terminal holding of other AA&E shipments, which are transported under Satellite Motor Surveillance Service (SNS), are published in items 312 and 314 of MFTRP No. I B.

Occasionally non-AA&E shipments may be transported under SNS, either alone or in combination with other protective services. These non-AA&E shipments moving under SNS will be afforded the required protection according to the TPS in addition to SNS. Also, when multiple shipments requiring different protective services are held in a terminal, the highest applicable protective service standard will apply.

Future questions and concerns regarding this issue may be addressed to Mr. Robert Jones, (703) 428-2308, FAX (703) 428-3347, or email: jonesr@mtmc.army.mil.

Francis A. Galluzzo
Director
Distribution Analysis Center

CF:
American Trucking Association, ATTN: Mr. William Wanamaker

HQ, Military Traffic Management Command, ATTN: Operations Center
MTMC Approved Transportation Protective Service Carriers

SECTION 4, PART A

ITEM

**TERMINAL STANDARDS FOR INTRANSIT HOLDING
OF SMALL SEUMENTS OF ARMS, AMMUNITION AND
EXPLOSIVES (AA&E) AND OTHER ITEMS TRANSPORTED
UNDER SATELLITE MOTOR SURVEILLANCE**

1. The below are the minimum required security standards for commercial carrier terminals to handle the following shipments transported under the protective services indicated:

Shipment Type

- Small quantity shipments of arms, ammunition and explosives (AA&E) (as defined in DTR, Part U, Chapter 205, Paragraph F)
- Classified, non-AA&E shipments
- Other sensitive or pilferable, non-AA&E shipments.

*Protective Service(s)***DOD Constant Surveillance Service (CIS)****Protective Security Service (PSS) or CIS****Dual Driver Protective Service (DDP) or CIS**

a. The carrier shall maintain a comprehensive facility security plan, evaluated by the Military Traffic Management Command (MTMC) during terminal inspections. The plan will address the specifics as to the terminal's implementation of the following standards:

(1) Access Control (2) Guard or employee observation. (3) Security cage (4) Lighting (5) Key and lock control (6) Communications (7) Employee Investigations

b. General: Terminal areas will have controlled access. When the terminal is attended by at least two terminal personnel, the classified or sensitive cargo will be under the specific observation of terminal employees involved in processing DOD cargo or be in a locked container or security cage. When the terminal is not constantly attended, the classified or sensitive DOD cargo shall be in a locked security cage or alternative container (see paragraph I c, below), and the terminal will be protected by a guard(s), IDS or CCTV.

c. Access Control: The terminal manager shall establish strict personnel and vehicle access control measures for the terminal area. At a minimum, photo identification cards will be required for all employees and worn during the performance of their official duties. Visitors and vendors will be logged in and out, and will either require escort or a temporary visitors badge which will be prominently displayed at all times prior to being granted access to the terminal. Visitor logs will be retained on file for a period of not less than one year and will be subject to audit during external reviews or inspections. DOD visitors will be pre-cleared by MTMC Fort Eustis, VA by calling the MTMC Customer Service Hotline at 1-800-524-033 1.

d. Guard or Employee Observation: Unattended terminals with classified or sensitive DOD shipments must be guarded or be locked and equipped with an IDS or CCTV that is linked to a response force capable of responding to the terminal location in accordance with the National Industrial Security Program Operating Manual (NISPOM) which calls for guards to meet 15-minute response time 80 percent of the time. However, carrier may request approval from MTMC to extend response time up to 30 minutes if mandated by environmental factors (e.g., traffic, distance). Where guards are used, the terminal shall maintain a minimum requirement of one guard per shift.

(1) Guard force personnel are not required to be armed. If the interior of the terminal area is not in full view of the guard, a second guard will be on site at all times, or the terminal will be equipped with an IDS or CCTV. If a CCTV system is used it must be linked to an alarm system that complies with the Underwriters Laboratory (UL) Standard 2050 and has received the UL Certificate of Compliance. In lieu of the second guard, a terminal employee may be used to provide attendance and surveillance of the DOD shipment.

(2) A guard shall patrol the terminal area at intervals not to exceed one-hour. The guard force will provide around-the-clock coverage.

(3) Guards shall be professionals; however, where terminal employees are used in lieu of a second guard, they are not required to be trained as professional guards. All employees involved in transporting a sensitive or classified DOD shipment are required to be trained on the sensitivity of the shipment and requirements for protecting the shipment from loss, theft or damage.

(4) Guards attending a terminal will be afforded formal training and provided specific standing operating procedures on security requirements for the terminal. At a minimum, training will encompass the responsibility and authority of security personnel, location

and use of first aid, fire control and any electronic security equipment. Guards will be educated on emergency planning and contingency response procedures, common tactics, and indicators of hostile intelligence, criminal and terrorist elements. They will be aware of the location and nature of classified, hazardous and sensitive equipment or material. Attending personnel other than guards will receive training on terminal security requirements, specific security and HAZMAT requirements for DOD shipments, emergency planning and contingency response procedures.

(5) Guards will be provided with equipment necessary to accomplish the security mission. They will have a direct communications link to either the carrier headquarters or commercial security service dispatcher at all times in case of emergency. Hourly communications checks will be performed after normal working hours. Additionally, they will be provided with a reliable secondary means of communication when conducting security checks/patrols of the surroundings.

e. Security Cages: A security cage holding sensitive or classified material must meet the following standards:

(1) General: Security cages will be fabricated from commercial steel grating panels. Walls, doors, floors, and ceiling must provide protection equivalent to the steel grating to preclude forced entry. Doors must have DOD approved padlocks (equivalent to American 200 series) and hasp systems and connecting hardware must be welded or otherwise secured to deter unauthorized entry.

(2) Walls: Constructed of structural steel angle and expanded steel grating. Building walls also may be used which provide equivalent security to form sides. (Example: Double-course reinforced or filled concrete block).

(3) Floors: Made of asphalt or reinforced concrete or wood if reinforced with steel floor plating.

(4) Ceiling: Same material as wall or floor. Minimum height: 8 feet. Frame: metal. Hinges: welded hinge pins. Locks: DOD approved (equivalent to American 200 series) security locks and hasps.

(5) Connecting Devices: Welded, peened, or otherwise installed so as to deter unauthorized entry.

(6) Windows/openings: Expanded steel grating, anchored in metal frame, secured in same manner as door.

(7) Alternative: As an alternative to a security cage, a CONEX, dromedary, or similar heavy container which is sealed and locked with a DOD-approved (equivalent to American 200 series) lock may be used in buildings which are locked and continuously attended, guarded, or equipped with CCTV/IDS. In lieu of locking the containers, they may be placed with doors against each other or against a substantive building wall.

(8) Locks securing non-AA&E classified material must be General Services Administration (GSA) approved and meet Federal Specification FF-L-2740 or FF-P- 110.

f. Lighting: Protective lighting shall be installed to discourage or deter attempts by intruders, make detection likely if entry is attempted and prevent glare that may temporarily blind guards or other personnel attending the terminal. Security lighting will be automatically timed and controlled to provide illumination from dusk until dawn. Lighting will not unnecessarily expose/silhouette guards or other personnel to targeting by criminal/terrorist elements. Lighting will illuminate the area beyond the perimeter to 20 feet beyond the outer edge of the terminal.

g. Key and Lock Control: Only DOD approved locks and locking devices will be utilized to safeguard unattended terminals holding DOD shipments and to protect DOD shipments temporarily stored in security cages or alternative containers. The terminal manager will establish a formal key and lock control system for those locks and locking devices. When unattended or not being used, keys and padlocks will be stored in a locked metal container or key depository. In the event of lost, misplaced, or stolen keys, the affected locks or locking devices will be replaced immediately. Lost keys will be immediately reported to the terminal manager or his/her designee. The use of a master key or multiple key system is prohibited. Keys will be signed out as needed to authorized employees on a key control register. A key and lock inventory will contain a record of keys, locks, key serial numbers, lock serial numbers, location and the number of keys maintained for each lock. This record will be maintained in the key depository. A 100% physical inventory of all keys and padlocks will be performed on a monthly basis. Documents used to control keys and locks will be retained on file for a minimum of one year and will be subject to audit during external reviews or inspections.

h. Communications: Communications shall provide a means of alerting local law enforcement and/or emergency response forces to the presence of intruders immediately. The terminal manager will identify and coordinate with the backup force capability.

i. Employee Investigation: The carrier shall establish a program to conduct pre-employment screening on employees. The checks shall cover the employee's complete employment history and a review of driving records to determine disqualifying violations under Department of Transportation rules. The carrier's security officer or equivalent will evaluate suitability for employment and will retain results in the employee's personnel file for review by MTMC and Defense Security Service (DSS). Employee records will be subject to review during authorized terminal inspections or as a part of an individual's security clearance process by DSS. MTMC Operations Center (757-878-7555/8141) will pre-approve access to terminal facilities and records by all inspectors.

2. The following are additional Security Requirements for Temporary Holding of SECRET (PSS) DOD Shipments:

- a. All terminal personnel having advance knowledge of and/or access to SECRET (PSS) shipments will hold a current SECRET clearance in accordance with the requirements of the National Industrial Security Program Manual (NISPOM).
- b. Terminal manager will coordinate with local, county or state law enforcement to provide additional security patrols of the terminal, including back-up forces, during higher threat periods as identified to the carrier by MTMC.

3. The following are safety Requirements for Terminals holding HAZMAT shipments.

- a. All terminal personnel responsible for processing AA&E and other HAZMAT shipments shall receive RAZMAT awareness training in accordance with requirements of Part 49 of the Code of Federal Regulation.
- b. HAZMAT training records will be subject to review during authorized terminal inspections



DEPARTMENT OF THE ARMY
HEADQUARTERS, MILITARY TRAFFIC MANAGEMENT COMMAND
200 STOVALL STREET HOFFMAN BUILDING 11
ALEXANDRIA VA 22332-5WO



March 14, 2002

Distribution Analysis Center

Munitions Carrier Industry

Policy Letter (PL) No. 2002-03: IN-TRANSIT PROTECTION REQUIREMENTS FOR FREIGHT OF ALL KIND (FAK) AND NON-SENSITIVE HAZARDOUS MATERIALS (HAZMAT) SHIPMENTS

The following provides guidance on the movement and in-transit handling of shipments with commodity descriptions or identified as FAK and other shipments of non-sensitive HAZMAT commodities that normally do not require special handling or transportation protective services.

Shipments identified as FAK and non-sensitive HAZMAT shipments normally do not require special transportation protective services. These shipments may be held in terminals that meet neither the standards in items 312 and 314 of MTMC Freight Traffic Rules Publication (MFTRP) No. I B nor the standards outlined in MTMC Policy Letter (PL) No. 2002-02. However, in accordance with Department of Transportation, state and local regulations, and item 130, MFTRP No. I B, the carrier is expected to take precautions to protect FAK and HAZMAT shipments from loss, pilferage, theft or damage during movement and at in-transit locations. In addition, HAZMAT shipments must receive proper safety handling and precautions in accordance with Part 49 of the Code of Federal Regulation.

Whenever multiple shipments are being held in the same location and require varying levels of protection or safety in a terminal, the most stringent applicable standard will apply. Compatibility requirements also apply for holding HAZMAT and arms, ammunition and explosives (AA&E) in the same terminal.

Francis A. Galluzzo
Director
Distribution Analysis Center

CF: American Trucking Association, ATTN: Mr. William Wanamaker HQ, Military Traffic Management Command,
ATTN: Operations Center MTMC Approved Transportation Protective Service Carriers